

学校编码：10384

分类号\_\_\_\_\_密级\_\_\_\_\_

学 号：X2010230271

UDC \_\_\_\_\_

厦 门 大 学

硕 士 学 位 论 文

# 图像加密与 LSB 水印技术及其 在基层电子政务安全中的应用

Methods of Image Encryption and LSB Watermarking and  
Its Application in the Security of Grass-root E-government

张方宁

指导教师姓名：刘昆宏 副教授

专 业 名 称：软 件 工 程

论文提交日期：2012 年 01 月

论文答辩时间：2012 年 05 月

学位授予日期：

答辩委员会主席：\_\_\_\_\_

评 阅 人：\_\_\_\_\_

2012 年 03 月

厦门大学博硕士论文摘要库

## 厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下,独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果,均在文中以适当方式明确标明,并符合法律规范和《厦门大学研究生学术活动规范(试行)》。

另外,该学位论文为( )课题(组)的研究成果,获得( )课题(组)经费或实验室的资助,在( )实验室完成。(请在以上括号内填写课题或课题组负责人或实验室名称,未有此项声明内容的,可以不作特别声明。)

声明人(签名):

年 月 日

## 厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（        ） 1.经厦门大学保密委员会审查核定的保密学位论文，  
于        年        月        日解密，解密后适用上述授权。

（        ） 2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年        月        日

## 摘要

随着电子政务应用的不断深入，使得政府部门的工作方式发生了巨大的变化。电子政务给政府工作带来方便和高效率的同时，也带来许多安全问题。街道社区作为最基层的政府部门，其电子政务建设同样面临着严峻的信息安全问题。信息被非法篡改，个人隐私被泄露以及各种数字作品被未经授权复制等非法现象时有发生。因此如何保证基层电子政务数字信息的安全已成为人们关注的重点。本文将分别从数字图像加密和数字水印这两个方面来阐述保障数字信息安全的方法。

在数字图像加密方面，本文从介绍密码学理论入手，然后介绍了数字图像的数学表示形式；根据数字图像的特性分析，明确对图像的加密不仅可以在空间域上展开，同时也可以从数字图像的变换域上进行；然后分类介绍了几种图像加密技术；对于数字图像加密的具体实现，本文详细介绍了三种方法，包括基于矩阵的 RGB 置乱加密，基于 Logistic 混沌映射的图像加密和基于 Arnold 置乱的图像加密。

在数字水印技术方面，首先阐述了数字图像水印技术的基本原理和它的分类；然后详细介绍了经典空间域数字水印算法——基于 LSB 的数字水印算法。

本文实现了以上相关算法，并展示了一个演示系统。在实现系统时，为了让该算法具有一定的鲁棒性，在算法实现时让水印信息均匀的分布在宿主图像中，并为了提高水印的安全性，对水印图像做了加密的预处理。

**关键字：**图像加密；数字水印； Arnold 变换；

## Abstract

With the deep development of E-government application, the modes of government workings change largely. But E-government brings security problems along with the high efficiency. As an important node, the E-government construction of Street Community also faces the severe security problems. Unauthorized tampered personal information, personal privacy leak and various unauthorized copy of digital works and other illegal phenomena happen often. Therefore, how to guarantee the safety of digital information has been a major concern. The dissertation respectively from the digital image encryption and digital watermark elaborates the information safety protection methods.

In the digital image encryption, the dissertation begins at the introduction of its theory, then with the mathematical representation of digital image; According to the characteristics of digital images, it shows that the image encryption can not only spread in spatial domain, also spread in the transform domain of digital image; Then it in classification introduces some image encryption technologies; For concrete implementation of digital image encryption, the dissertation introduces three kinds of methods, including matrix based RGB scrambling encryption, Logistic chaos system based image encryption and Arnold transformation based image encryption.

In digital watermarking technology, it first expounds the basic principles of technology and classification of digital image watermarking; then introduces classic space domain digital watermarking algorithm - LSB watermarking algorithm. In order to achieve certain robustness in the algorithm, the dissertation lets watermarking information evenly distributed in host image, and in order to improve the security of watermark, making encryption preprocessing to the watermark image.

**Keywords:** Image Encryption; Digital Watermark; Arnold Transformation;

## 目 录

<b>第一章</b>	<b>绪论 .....</b>	<b>1</b>
1.1	课题研究的背景和意义 .....	错误！未定义书签。
1.2	研究历史与现状 .....	3
1.3	研究内容 .....	6
1.4	论文组织结构 .....	7
<b>第二章</b>	<b>数字图像加密技术概述 .....</b>	<b>9</b>
2.1	密码学综述 .....	9
2.1.1	密码学系统 .....	9
2.1.2	密码学分类 .....	10
2.2	数字图像加密技术简介 .....	12
2.3	图像加密技术 .....	13
2.3.1	基于矩阵变换及像素置换的图像加密技术 .....	14
2.3.2	基于秘密分割与秘密共享的图像加密技术 .....	14
2.3.3	基于现代密码体制的图像加密技术 .....	15
2.3.4	基于混沌的图像加密算法 .....	15
2.3.5	基于变换域的加密方法 .....	16
2.4	本章小结 .....	16
<b>第三章</b>	<b>数字水印技术概述 .....</b>	<b>17</b>
3.1	信息隐藏技术原理 .....	17
3.2	数字水印技术的基本原理 .....	18
3.3	数字水印技术的分类及常用的算法 .....	19
3.3.1	空间域数字水印 .....	19
3.3.2	频域数字水印 .....	20
3.4	本章小结 .....	20
<b>第四章</b>	<b>数字图像加密和解密实现 .....</b>	<b>21</b>
4.1	基于矩阵的 RGB 置乱加密和解密 .....	21
4.1.1	彩色图像的 RGB 颜色空间 .....	21
4.1.2	算法描述 .....	21
4.1.3	算法实现 .....	23
4.1.4	实验结果 .....	25
4.2	基于 Logistic 混沌映射的图像加密和解密 .....	26
4.2.1	Logistic 映射概述 .....	26
4.2.2	算法描述与实现 .....	28

4.2.3 实验结果.....	30
<b>4.3 基于 Arnold 置乱的图像加密和解密.....</b>	<b>31</b>
4.3.1 Arnold 变换 .....	31
4.3.2 算法描述与实现.....	32
4.3.3 实验结果.....	34
<b>4.4 组合加密 .....</b>	<b>35</b>
<b>4.5 图像加密效果评价 .....</b>	<b>36</b>
4.5.1 主观评价 .....	36
4.5.2 客观评价 .....	37
<b>4.6 本章小结 .....</b>	<b>39</b>
<b>第五章 基于 LSB 的数字水印实现.....</b>	<b>40</b>
5.1 LSB 数字水印 .....	40
5.2 算法描述与实现.....	40
5.3 实验结果 .....	42
5.4 本章小结 .....	46
<b>第六章 图像加解密与 LSB 水印技术在电子政务安全中的应用 ..</b>	<b>47</b>
6.1 系统应用背景分析.....	错误！未定义书签。
6.2 应用业务流程分析 .....	52
6.3 系统设计 .....	51
6.3.1 系统开发工具的选择.....	52
6.3.2 原型系统的功能结构.....	53
6.3.3 系统界面设计.....	37
6.4 系统实现.....	53
6.4.1 辅助结构及工具函数.....	54
6.4.2 图像加密和解密功能实现.....	55
6.4.3 水印嵌入和水印提取的功能实现.....	56
6.5 系统应用结果 .....	59
6.5.1 图像加解密技术的应用.....	56
6.5.2 水印嵌入和提取技术的应用.....	57
6.5.3 水印加密嵌入和提取技术的应用.....	58
6.6 本章小结 .....	59
<b>第七章 总结与展望 .....</b>	<b>60</b>
7.1 总结 .....	60
7.2 工作展望 .....	61
<b>参考文献 .....</b>	<b>62</b>
<b>致谢.....</b>	<b>63</b>



## Contents

<b>Chapter 1 Introduction.....</b>	<b>1</b>
1.1 Research Backgrounds.....	错误！未定义书签。
1.2 History and Recent Status .....	3
1.3 Main work of this Dissertation.....	6
1.4 Organization of this Dissertation .....	7
<b>Chapter 2 Overview to Image Encryption .....</b>	<b>9</b>
2.1 Introduction to Cryptography.....	9
2.1.1 Cryptography System.....	9
2.1.2 Cryptography Classification .....	10
2.2 Digital Image Encryption Sketch.....	12
2.3 Technologies of Image Encryption.....	13
2.3.1 Matrix Transform and Pixel Permuting Based Image Encryption...	13
2.3.2 Confidential Division and Sharing Based Image Encryption .....	14
2.3.3 Modern Cipher Structure Based Image Encryption.....	15
2.3.4 Chaos Based Image Encryption Algorithm.....	15
2.3.5 Transforming Domain Based Encryption .....	16
2.4 Summary .....	16
<b>Chapter 3 Overview to Watermarking Technology.....</b>	<b>17</b>
3.1 Information Hiding Principles .....	17
3.2 Basic Principles of Watermarking Technology .....	18
3.3 Classification and Usual Algorithms of Watermarking Technology....	19
3.3.1 Space Domain Digital Watermarking .....	19
3.3.2 Frequency Transforming Domain Watermarking .....	20
3.4 Summary .....	20
<b>Chapter 4 Digital Image Encryption and Decryption.....</b>	<b>21</b>
4.1 Matrix Based RGB Scrambling Encryption and Decryption .....	21
4.1.1 RGB Color Model.....	21
4.1.2 Algorithm Description .....	21
4.1.3 Algorithm Implementation.....	23
4.1.4 Experimental Result.....	25
4.2 Logistic Chaos System Based Image Encryption and Decryption.....	26
4.2.1 Logistic Chaos System Sketch.....	26
4.2.2 Algorithm Description and Implementation .....	28

4.2.3	Experimental Result.....	30
<b>4.3</b>	<b>Arnold Transformation Based Image Encryption and Decryption .....</b>	<b>31</b>
4.3.1	Arnold Transformation.....	31
4.3.2	Algorithm Description and Implementation .....	32
4.3.3	Experimental Result.....	34
<b>4.4</b>	<b>Combination Encryption .....</b>	<b>35</b>
<b>4.5</b>	<b>Evaluation of Image Encryption .....</b>	<b>36</b>
4.5.1	Subjective Evaluation .....	36
4.5.2	Objective Evaluation.....	37
<b>4.6</b>	<b>Summary .....</b>	<b>39</b>
<b>Chapter 5</b>	<b>Implementation of LSB Based Watermarking .....</b>	<b>40</b>
<b>5.1</b>	<b>LSB Based Watermarking Introduction .....</b>	<b>40</b>
<b>5.2</b>	<b>Algorithm Description and Implementation.....</b>	<b>40</b>
<b>5.3</b>	<b>Experimental Result.....</b>	<b>42</b>
<b>5.4</b>	<b>Summary .....</b>	<b>46</b>
<b>Chapter 6</b>	<b>Technologies Applications in Security of E-government...47</b>	
<b>6.1</b>	<b>OpenCV Sketch .....</b>	<b>错误！未定义书签。</b>
<b>6.2</b>	<b>Function Structure of Demonstrating System .....</b>	<b>529</b>
<b>6.3</b>	<b>System Design .....</b>	<b>51</b>
6.3.1	OpenCV Sketch .....	52
6.3.2	Function Structure of Demonstrating System.....	53
6.3.3	Interface Design .....	53
<b>6.4</b>	<b>System Implementation .....</b>	<b>53</b>
6.4.1	Auxiliary Structure and Tool Function .....	554
6.4.2	Function Implementation of Image Encryption and Deciphering ...	55
6.4.3	Function Implementation of Watermarking Implant and Extract ....	56
<b>6.5</b>	<b>Application Results.....</b>	<b>59</b>
6.5.1	Applications of Image Encryption and Deciphering .....	56
6.5.2	Applications of Watermarking Implant and Extract .....	56
<b>6.6</b>	<b>Summary .....</b>	<b>59</b>
<b>Chapter 7</b>	<b>Conclusions and Future Work.....</b>	<b>60</b>
<b>7.1</b>	<b>Conclusions .....</b>	<b>60</b>
<b>7.2</b>	<b>Future Work.....</b>	<b>61</b>
<b>References</b>	<b>.....</b>	<b>62</b>
<b>Acknowledgements</b>	<b>.....</b>	<b>63</b>

## 第一章 绪论

### 1.1 课题研究的背景和意义

电子政务（E-government）是指政府机构应用现代信息和通信技术，将管理和服务通过网络技术进行集成，在互联网上实现政府组织结构和工作流程的优化重组，超越时间、空间与部门分隔的限制，全方位地向社会提供优质、规范、透明、符合国际水准的管理和服务。从结构上看，电子政务是一个由内网（包括核心数据层和办公业务层）、外网（公众服务）和互联网（数据交换层）三级网络构成的庞大的信息系统。

随着全球政治、经济一体化步伐的加快，以电子政务为代表的政府管理服务职能的电子化、自动化、无纸化正在一些国家，尤其是发达国家中兴起。我国自实施“政府上网计划”以来，各级政府的电子政务建设发展很快。由于电子政务依赖于计算机和网络技术这一平台而存在，就意味着其应用不可避免地存在着由于 Internet 的自由、开放所带来的信息安全隐患<sup>[1]</sup>。网络构成的虚拟社会一直都不安宁，网上个人信息的被泄露、篡改和假冒，黑客入侵，计算机犯罪，计算机病毒传播等不良行为时常发生，对网络信息形成了重大威胁。因此信息的安全问题显得越来越突出，信息安全技术也正越来越受到全社会的普遍关注。信息安全技术不但关系到个人通信的隐私问题，还关系到一个企业的商业机密和企业的生存问题，甚至关系到一个国家的安全问题<sup>[2]</sup>。

信息安全主要体现在信息的保密性、完整性、可用性这三个方面<sup>[3]</sup>。其中，保密性是指对信息的存储、传输进行保护，确保信息不泄露给未经授权的个人、实体和进程，或供其使用的特性；完整性是指保护信息不遭到非授权的修改、破坏；可用性是指合法用户访问并能按要求顺序使用信息的特性，即保证合法用户在需要时可以访问到信息及相关资产。另外信息安全还包括可控制性和抗审查性。

信息安全的核心技术是信息加密技术。本文从数字图像加密和数字水印这两

个方面来阐述保障数字信息安全的方法：

(1) 信息可以通过符号、文本，数据，语音，图像，视频等多种形式来表达。在不同的情况下，人们总是会根据当时的条件合理运用这些表达形式来进行交流。其中，图像是具有直观、形象和生动优点的信息表达形式。同时，随着计算机网络和多媒体等技术的迅猛发展，数字图像克服了以往因图像数据量大而带来的存储和传输问题，它正在或者已经成为一种主流的信息表达方式<sup>[4]</sup>。在人们的日常生活中，图像的使用也伴随着人们，如数码摄像，手机拍照，QQ 视频和在网络中分享的各种照片等都与图像息息相关。由于数字图像使用的方便性和广泛性，图像信息的安全也受到了强大的威胁。信息一旦出现在网络上，它将被轻易地获取，对原始信息的非法复制和未经授权的传播，导致个人隐私的泄露，以及蓄意修改个人信息都会带来严重的后果。这样在人们享受图像给生活带来诸多便利的同时，也越来越关注保障数字图像安全的方法。如何保障数字图像信息的安全是国际上热门的研究课题之一。图像加密技术是保障数字图像信息安全措施的一个重要分支，它是一个结合了数学、密码学、信息论、计算机视觉以及其它计算机应用技术的多学科交叉的研究课题。

(2) 信息安全技术经过多年的发展，已经从密码技术发展到了隐藏技术<sup>[2]</sup>。信息隐藏技术就是把机密信息隐藏在含有大量信息的其他媒体（如音频，视频，图像）中，通过载体的传输，实现机密信息的传递。信息隐藏技术通常以某种媒体作为载体，将机密信息嵌入到其中，以一种只有授权者才知道信息存在的秘密途径传送信息。虽然信息隐藏与信息加密都是致力于信息的保密技术，但是，两者的设计思想完全不同。信息加密主要通过设计加密技术，使保密信息不可读，但是对于非授权者来说，虽然他无法获知保密信息的具体内容，但却能意识到保密信息存在；而信息隐藏则致力于通过审计精妙的方法，使得非授权者根本无从得知保密信息存在与否。相对于现代密码学来讲，信息隐藏的最大优势在于它并不限制对主信号（载体）的储存和访问，而是致力于签名信号的安全保密性<sup>[6]</sup>。作为信息隐藏技术的一个重要分支，数字水印技术就是近年来比较热门的数字产品版权保护技术。

## 1.2 研究历史与现状

### 1.2.1 电子政务安全现状

电子政务的网络应用系统必然涉及到国家和本单位的秘密，涉及到多种敏感数据和各类重要文件，因此对安全保障系统有非常高的要求。进而言之，电子政务系统信息安全的宗旨就是通过在实现信息系统时充分考虑信息风险，从而确保一个政府部门能够有效地完成法律所赋予的政府职能。电子政务面临的威胁导致了对电子政务安全的需求，也是真正实现一个安全电子政务系统所要求做到的各个方面，主要包括机密性、完整性、认证性、不可抵赖性和有效性：

（1）机密性。电子政务作为政府服务的一种手段，直接代表着个人、机构或国家的机密。电子政务是建立在一个较为开放的网络环境，维护政府机密是电子政务全面推广应用的重要保障。因此，要预防非法的信息存取和信息在传输过程中被非法窃取。机密性一般通过密码技术来对传输的信息进行加密处理来实现。

（2）完整性。电子政务简化了服务过程，减少了人为的干预，同时也带来维护各方信息的完整、统一的问题。由于数据输入时的意外差错或欺诈行为，可能导致各方信息的差异此外，数据传输过程中信息的丢失、信息重复或信息传送的次序差异也会导致各方信息的不同。各方信息、的完整性将影响到各方对电子政务的满意度，各方信息的完整性是电子政务应用的基础。因此，要预防对信息的随意生成、修改和删除，同时要防止数据传送过程中信息、的丢失和重复并保证信息传送次序的统一。完整性一般可通过提取信息消息摘要的方式来获得。

（3）认证性。由于电子政务系统的特殊性，政务活动通常都是在虚拟的网络环境中进行，所以对个人或机构实体进行身份性确认成了电子政务中很重要的一环对人或实体的身份进行鉴别，为身份的真实性提供保证，即双方能够在相互不见面的情况下确认对方的身份。这意味着当某人或实体声称具有某个特定的身份时，鉴别服务将提供一种方法来验证其声明的正确性，一般都通过认证机构CA和证书来实现。

（4）有效性。电子政务以电子形式取代了纸张，那么如何保证这种电子形

式的信息的有效性则是开展电子政务的前提电子政务作为政务的一种形式,其信息的有效性将直接关系到个人、机构或国家的利益和声誉。因此,要对网络故障、操作错误、应用程序错误、硬件故障、系统软件错误及计算机病毒所产生的潜在威胁加以控制和预防,以保证数据在确定的时刻、确定的地点是有效的。

(5) 不可抵赖性。如何确定要进行服务的服务对象是进行服务所期望的服务对象这一问题则是保证电子政务顺利进行的关键。要在政务信息的传输过程中为参与政务活动的个人、机构或国家提供可靠的标识。不可抵赖性可通过对发送的消息、进行数字签名来获取。

然而,我国电子政务面临的安全现状不容乐观,特别是在基层政府机关,其电子政务的安全堪忧,如:电子政务信息系统存在网络缺陷及软件漏洞问题,因黑客恶意攻击或病毒传播导致的安全问题,数据泄漏或用户验证导致的安全问题,管理欠缺等。除了这些一般性安全问题之外,我国的电子政务系统还存在众多额外的安全隐患,那就是我国的各级政府部门目前所选用的高端软硬件平台,基本上都是国外公司的产品。近些年来,国外公司技术垄断所造成的危害,已经逐步显现。如何建设和完善电子政务安全,以满足政府服务大众,提高行政效率,推进电子政务的发展,是我们面临的紧迫的课题。从长远来看为保证我国电子政务的正常发展,对电子政务安全进行研究,发展自主的电子政务安全技术是十分必要的。

总之,安全是电子政务的核心,其重要性毋庸置疑。电子政务安全首先是国家安全问题,安全是国家的根本利益所在。电子政务安全是国家各种利益得以保证的基础,发展电子政务是政府转变职能、转换运行机制、提高行政效率、增加行政管理透明度、促进政府信息资源共享方面的共同需求,所代表的不仅是政府部门的利益,更代表企业和公众的利益电子政务安全是社会稳定的基本保障,电子政务大大增强了政务的社会服务职能,使企业的经营和公众的生活越来越依赖电子政务系统的安全运行,一旦某环节出问题,势必造成社会秩序的混乱。我们要坚持引进、吸收的前提下,组织各方面力量,自主研制和开发具有独立知识产权信自、安全产品,制定符合我国国情的电子政务安全的行政法规,逐步掌握信息、安全核心技术,并从宏观上加以调控,为我国电子政务发展构筑安全的屏障。

### 1.2.2 图像加密和数字水印发展现状

数字图像加密技术源于早期的经典密码学理论<sup>[2]</sup>。密码学的发展由来已久，其历史可以追溯到几千年以前。加密最终目的就是将信息隐藏起来，对未授权的人保留信息的真实含义。早在四千多年以前，古埃及人就开始使用密码技术来保密要传递的消息。一直到第一次世界大战前，密码技术的进展很少公布，直到1918年，William F. Friedman 的论文“The Index of Coincidence and Its applications in Cryptography”发表时，情况才有所好转。在这段漫长的时期内，信息的保密基本上靠人工对消息加密、传输和防破译；其应用也主要限制于军事目的，只为少数人掌握和控制。所以，它的发展受到了限制。1949年，保密系统的通信理论的发表为密码技术奠定了坚实的理论基础，使密码学真正成为了一门学科。1976年，W.E. Diffie 和 M.E. Hellman 发表了《New Direction in Cryptography》一文，提出了一种全新的密码设计思想，并首次证明了在发送端和接受端不需要传送密钥的保密通信是可能的，从而开创了公钥密码技术的新纪元，成为现代密码技术的一个里程碑。1977年美国国家标准局 NBS 正式公布了数据加密标准 DES，将 DES 算法公开，从而促进了 DES 的推广。1978年第一个最成熟的，也是迄今为止理论上最成功的公钥密码体制——RSA 公钥密码技术实现。1984年一种基于量子定律的密码技术——BB84 协议被提出，它是一种具有发现窃听等攻击行为和抗击具有无限计算能力攻击功能的密码学技术。1985年公钥密码技术中成功运用那个了椭圆曲线卢纶，成为了公钥密码技术研究的新亮点。与此同时，密码技术的另一个重要方向——序列密码理论也取得了重大的进展。1989年，序列米娜及保密通信理论使用了混沌理论，为序列密码的研究开辟了一条新的途径。80年代以来，密码学的研究如雨后春笋般进入了全面发展阶段，一系列的密码协议与密码算法相继产生。2000年，新的加密技术标准 AES 颁布，取代了 DES 算法。

在网络技术与多媒体技术飞速发展的影响下，信息的安全和保密变得尤为重要，而数字图像作为信息表达较为形象生动和直接的一种形式，如何保障其安全性也是当前的热门研究课题之一。传统的密码学着眼于文本资料的加密处理，为数字图像的加密提供了最直接的理论依据，但是它常常考虑的是二进制流，忽略

了图像的视觉效果。数字图像数据量大，要求加密具有实时性，传统的加密方法并不适合；传统的计算机图形学着眼于图形图像的数字生成，又忽略了对图像的安全性研究<sup>[1]</sup>。

对于数字图像，有两种有效的保护技术<sup>[7]</sup>。其一是近年来发展起来的数字水印技术。通过在数字图像中嵌入数字水印信息可以较为有效的实现数字图像版权保护，但这样的图像并不改变图像的可见性，这对娱乐工业中涉及知识产权的鉴定或许是可行的，但对于某些特殊的通信场合，例如军用卫星摄取的图片、患者的病历等的传输以及娱乐工业中产品的网络发送等是不合适的。其二是图像加密技术。通过图像加密操作后，原来的数字图像变为类似于信道随机噪声的信息，这些信息对不知道密钥的网络窃听者是不可识别的（除非进行了有效破译），进而可以有效地保护传输中的图像数据。随着人们对知识产权的重视及娱乐工业的发展，可以预见，图像加密技术会有广阔的应用前景。

近年来，针对数字图像数据量大这一特点，许多关于的图像加密算法出现<sup>[2]</sup>。按加密时有无数据压缩可分为两大类，即加密的同时有数据压缩及只有加密而无数据压缩两类。而按加密的对象来分，也可分为两类：一类是直接对图像数据进行加密；另一类则是对图像数据编码的辅助信息进行加密。而按加密的手段来讲也可分为两大类：一类是应用图像数据的特点，再加上现代密码技术来达到加密的目的，如先对图像数据进行编码，再对编码信息进行加密；另一类是建立一种完全新式的密码体制来达到对图像数据加密的目的，如应用混沌动力系统加密图像数据。这些分类方法实际体现在某一具体的算法上时是相互交叉的，只是看问题的角度不同而已。具体来讲主要有以下几种技术：基于置乱的图像加密技术；基于伪随机序列的加密技术；基于 SCAN 语言的加密技术；基于“密钥图像”的加密技术；基于二叉树编码及 SCAN 语言的加密技术；基于图像的矢量量化压缩编码技术及商业密码加密技术等等。

### 1.3 研究内容

我国地方政府机构中，基层电子政务的建设是至关重要的，处在整个国家电子政务体系的核心位置。因此，本文将以基层电子政务安全建设为研究背景，分



Degree papers are in the "[Xiamen University Electronic Theses and Dissertations Database](#)". Full texts are available in the following ways:

1. If your library is a CALIS member libraries, please log on <http://etd.calis.edu.cn/> and submit requests online, or consult the interlibrary loan department in your library.
2. For users of non-CALIS member libraries, please mail to [etd@xmu.edu.cn](mailto:etd@xmu.edu.cn) for delivery details.

厦门大学博硕士论文摘要库